IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

CENTRIPETAL NETWORKS, LLC,
Plaintiff,

v. Civil Action No. 2:18-cv-00094 (EWH)

CISCO SYSTEMS, INC.,
Defendant.

MEMORANDUM ORDER

This matter is before the Court on Plaintiff Centripetal Networks, LLC's Motion for Additional and Amended Findings and Amended Judgment under Rule 52(b), or, in the Alternative, For a New Trial Under Rule 59(a)(2) (the "Motion"). ECF No. 787. For the reasons below, the Motion is DENIED.

On December 11, 2023, this Court entered a Memorandum Opinion and Order ("Opinion") finding that Centripetal had failed to meet its burden to establish infringement by Defendant Cisco Systems, Inc. of U.S. Patent Nos. 9,686,193 ("the '193 Patent"); 9,203,806 ("the '806 Patent"); and 9,560,176 ("the '176 Patent"). ECF No. 780. The Court determined that because Centripetal had not met its burden in establishing infringement, it was not necessary to reach issues related to patent validity or damages. *Id.* at 1. The following day, the Clerk entered partial final judgment in favor of Cisco, and thereafter Centripetal timely filed this Motion for relief. ECF No. 781.

I. LEGAL STANDARD

Rule 52(b) of the Federal Rules of Civil Procedure provides that "[o]n a party's motion filed no later than 28 days after the entry of judgment, the court may amend its findings—or make additional findings—and may amend the judgment accordingly." Fed. R. Civ. P. 52(b). Likewise, under Rule 59(a)(2), "[a]fter a nonjury trial, the court may, on motion for a new trial, open the

judgment if one has been entered, take additional testimony, amend findings of fact and conclusions of law or make new ones, and direct the entry of a new judgment." Fed. R. Civ. P. 59(a)(2).

In patent cases, the standard applied when determining whether relief should be granted under Rule 52(b) or Rule 59(a)(2) is governed by the law of the regional circuit. *Bettcher Indus., Inc. v. Bunzl USA, Inc.*, 661 F.3d 629, 638 (Fed. Cir. 2011); 9C Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure* § 2582 (3d ed. Supp. 2024). The United States Court of Appeals for the Fourth Circuit has previously recognized three grounds for amending an earlier judgment: "(1) to accommodate an intervening change in controlling law; (2) to account for new evidence not available at trial; or (3) to correct a clear error of law or prevent manifest injustice." *Pac. Ins. Co. v. Am. Nat. Fire Ins. Co.*, 148 F.3d 396, 403 (4th Cir. 1998). "It is not the intention or purpose of Rules 52(b) and 59(e) to permit parties to relitigate old matters, or give an unhappy litigant one additional chance to sway the judge." *Floyd v. City of Spartanburg S.C.*, No. 7:20-CV-01305-JDA, 2024 WL 771047, at *2 (D.S.C. Feb. 26, 2024) (cleaned up); *see also Blick v. Shapiro & Brown, LLP*, 2018 WL 9619434, at *1 (W.D. Va. Aug. 10, 2018) ("A party who failed to prove his strongest case is not entitled to a second opportunity to litigate a point, to present evidence that was available but not previously offered, or to advance new theories by moving to amend a particular finding of fact or a conclusion of law." (quotation marks and citations omitted)).

II. DISCUSSION

Centripetal asks the Court to either reverse the judgment and find that Cisco infringed each of the three patents or reopen the case to allow for the presentation of additional evidence. In support of this extraordinary remedy, Centripetal contends that the Court committed "clear errors of fact and law" in its prior decision. Mem. in Supp. at 1, ECF No. 788. Plaintiff attributes these

purported errors, in large part, to the unique posture of this case, in which the undersigned applied Rule 63 of the Federal Rules of Civil Procedure to adjudicate the dispute using the trial record developed by a different judge.

As a brief background, in 2020, the Honorable Henry Coke Morgan, Jr. conducted a six-week bench trial via videoconference. Op. at 1. Judge Morgan ruled in favor of Centripetal, finding that Cisco's accused technology infringed the '193, '806, '176, and '856 Patents.[1] *Id.* Cisco appealed. Without reaching the merits, the Federal Circuit vacated Judge Morgan's infringement ruling and denial of Cisco's motion for a new trial. *Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 38 F.4th 1025, 1030–33, 1040 (Fed. Cir. 2022). The Court remanded the case for further proceedings before a new judge and directed that the proceedings be conducted pursuant to Federal Rule of Civil Procedure 63. *Id.* at 1040. Rule 63 provides that "[i]f a judge conducting a hearing or trial is unable to proceed, any other judge may proceed upon certifying familiarity with the record and determining that the case may be completed without prejudice to the parties." Fed. R. Civ. P. 63. The Rule also states that "[i]n a hearing or a nonjury trial, the successor judge must, at a party's request, recall any witness whose testimony is material and disputed and who is available to testify again without undue burden." *Id.*

Following remand, both parties submitted their respective positions on how the case should proceed. ECF Nos. 656, 657. Centripetal requested that the case be decided "based on the current record," and noted that recalling witnesses would be "unnecessary and wasteful." Pl.'s Notice at 1–2, ECF No. 656. In its post-trial motion, however, Centripetal now seeks to reopen the record and allow new testimony and evidence. Centripetal contends this approach is warranted because

[1] Following remand, the Court stayed the proceedings with respect to U.S. Patent No. 9,917,856 ("the '856 Patent") due to the PTAB's issuance of a final written decision declaring the '856 Patent claims asserted by Centripetal unpatentable. ECF No. 715; *see also* ECF No. 686.

the Court "altered the settled understanding of the constructions reached by the initial presiding judge." Mem. in Supp. at 1–2. Because the Court concludes that the claim language—as construed in the February 2020 claim construction order—was applied without modification, and that Centripetal fails to provide any other compelling reason for the Court to modify its judgment, it denies Centripetal's Motion.

A. '193 Patent

In its Opinion, the Court found that the Accused Switches and Routers[2] did not infringe claims 18 or 19 of the '193 Patent. Op. at 24–30. Claim 18 of the '193 Patent describes a system that first "receive[s] . . . a plurality of packets" from a "computing device" in a "first network." '193 Patent at 14:5–6. Then, if the packets are "destined for [a] second network," and the system makes a "determination that the . . . portion of packets comprises data corresponding to [rule] criteria . . . configured to prevent a particular type of data transfer from the first network to [the] second network," an operator is applied that is "configured to drop packets associated with the particular type of data transfer." *Id.* at 14:9–22. Alternatively, if the packets are "destined for a third network" and the system makes a "determination that the . . . packets comprise[] data that does not correspond to the [rule] criteria," an operator is applied that is "configured to forward packets not associated with the particular type of data transfer to the third network." *Id.* at 14:23–36. Claim 19 describes the same technique. *See id.* at 14:37–15:2; *see also* Op. ¶¶ 6–7.

The Court held that Centripetal failed to prove infringement because it could not show that the accused devices drop or forward packets based on the "particular type of data transfer." Op. at 24. In its post-trial motion, Centripetal (1) argues that the Court's analysis relied on a new, flawed

[2] Capitalized terms not defined herein are defined in the Court's Memorandum Opinion. ECF No. 780.

construction of "particular type of data transfer from [a] first network to a second network," and advocates that the Court find infringement under an alternate construction of the term; (2) requests that if the Court "adheres to its new construction," the record be reopened and Centripetal be allowed the opportunity to present new evidence; and (3) argues that the Court's decision included erroneous factual findings regarding the operation of Cisco's Accused Switches and Routers.

1. Claim Construction

Centripetal's first argument focuses on the Court's analysis of claim language requiring packet filtering of a "particular type of data transfer." As an initial matter, Centripetal never requested that this Court construe the term "particular type of data transfer"—during the *Markman* process or any time prior to entry of the judgment. The Court was therefore entitled to apply the plain and ordinary meaning of the term and Centripetal has "waived its right to [now] request a construction." *Eli Lilly & Co. v. Aradigm Corp.*, 376 F.3d 1352, 1360 (Fed. Cir. 2004); *see Conoco, Inc. v. Energy & Env't Int'l, L.C.*, 460 F.3d 1349, 1359 (Fed. Cir. 2006) ("[L]itigants waive their right to present new claim construction disputes if they are raised for the first time after trial."). Indeed, "[i]t is the parties' obligation to raise a dispute regarding the proper scope of claims to the court." *ATEN Int'l Co., Ltd. v. Uniclass Tech. Co., Ltd.*, 932 F.3d 1364, 1370 (Fed. Cir. 2019). Failure to do so is an implicit concession that the term is "clear and not in need of construction." *Eli Lilly & Co*., 376 F.3d at 1360. The Court was therefore entitled to presume that Centripetal chose not to propose a construction of the term "because one of ordinary skill in the art would understand [its] plain meaning[]." *Unitherm Food Sys., Inc. v. Swift-Eckrich, Inc.*, 375 F.3d 1341, 1350 (Fed. Cir. 2004), *rev'd in part on other grounds*, 546 U.S. 394 (2006).

Applying the plain and ordinary meaning of "particular type of data transfer," the Court found that Cisco's Accused Switches and Routers did not infringe claims 18 and 19 of the '193

Patent. The evidence showed that when Cisco's Accused Switches and Routers receive packets containing scalable group tags ("SGT" tags), they apply certain rules to the packets—specifically, Security Group Access Control Lists ("SGACLs"). *Id.* ¶¶ 11–12. SGT tags are appended to all of the packets transmitted by computers in a defined security group, and each SGT tag is associated with a different SGACL, which contains instructions as to how the packet should be treated. *Id.* ¶ 12. One such security group is the "quarantine" group. *Id.* ¶¶ 12, 15. All packets transmitted from quarantined computers are appended with a quarantine SGT tag, and when the packets pass through the Accused Switches and Routers, the devices apply the quarantine SGACL, causing the packets to be forwarded or dropped depending on their destination. *Id.* ¶ 15.

Moreover, "[a]lthough Centripetal alleged that the Accused Switches and Routers infringe the asserted claims of the '193 Patent based on the use of SGACL rules and SGT tags generally, at trial it focused only on their use in effecting a quarantine." *Id.* ¶ 14. Accordingly, the Court based its infringement analysis on the quarantine functionality. Two important factual findings regarding the operation of the quarantine rules drove the Court's conclusion: (1) that *all* packets transmitted from a computer in the quarantine group are appended with the quarantine SGT tag, and (2) that the quarantine SGACL instructs an Accused Switch or Router to either drop or forward a packet containing a quarantine SGT tag based on the packet's destination. *Id.* ¶¶ 15–18. "In other words, the quarantine rule can be set up to block a computer from accessing specific endpoints, such as part of a network containing sensitive company documents, while allowing access to other destinations, like the Internet." *Id.* ¶ 16.

The Court found this functionality—forwarding or dropping *all* packets from a computing device depending on what network that device is attempting to access—did not meet the "particular type of data transfer" limitation described in claims 18 and 19 of the '193 Patent. The

claims require that "two conditions must be met: (1) the packets from a device in a first network must be 'destined for [a] second network' and (2) the packets must meet rule criteria 'configured to prevent a particular type of data transfer from the first network to [the] second network.'" *Id.* at 25 (alterations in original) (quoting '193 Patent at 14:9–16). The Court concluded that, at a minimum, the reference to "particular type of data transfer" in the claim must refer to a *subset* of the packets from the "computing device" in the "first network" that are "destined for [a] second network." *Id.* at 24–29. The reason is simple—if *all* packets from the computing device satisfied the "particular type of data transfer" condition, the condition would be rendered superfluous. *Id.* at 25 (citing *W.L. Gore & Assocs., Inc. v. Medtronic, Inc.*, 834 F. Supp. 2d 465, 477 (E.D. Va. 2011)). Moreover, the notion that "particular type" does not mean "all types" is obvious and aligns with the plain and ordinary usage of the term. Therefore, because evidence showed that "the Accused Switches and Routers . . . drop *all* packets from a quarantined computer to a restricted network destination and allow *all* packets from a quarantined computer to a permitted network destination," Centripetal failed to meet the "particular type of data transfer" condition required by the claims. *Id.* at 23, 25.

In its post-trial motion, Centripetal takes issue with this analysis, suggesting that the Court improperly focused on filtration of "a subset of packets sent between *computers* in two different networks," while the claims merely disclose "filtering a subset of data *transfers* between two different *networks*." Mem. in Supp. at 5 (emphasis in original). The Court takes Centripetal to be suggesting the possibility that the packets received from the "computing device" in the first network described in the claim language could originate from multiple source computers in that network. *Id.* at 5–8. In that scenario, Centripetal appears to be claiming that a "particular type of data transfer" could refer not to a subset of the packets sent from a single quarantined computer,

but instead to the subset of packets that originated from quarantined computers as compared to non-quarantined computers. *Id.* at 8 (explaining that Cisco's devices infringe because they are able to "block certain *computers* in the first network—namely those that have been assigned a 'quarantine' SGT tag—from transferring packets to a second network") (emphasis added).

The Court finds that further clarification is necessary. In its ruling, the Court couched its analysis within a framework in which the first network packets *originated* from the computing device. The necessary implication was that the "computing device" was an endpoint computer in the first network—one that either was, or was not, subject to a quarantine.[3] As explained above, Centripetal's infringement theory focused on the quarantine functionality of the accused devices, in which quarantine SGT tags are used to restrict the network access of a quarantined computer. The Court rejected Centripetal's argument that SGT-tagged packets constitute a "particular type of data transfer" from the first network computing device (*i.e.*, the quarantined computer) because that would mean blocking or allowing *all* of the data transfers between the device and the second network. Op. at 27.

As Centripetal's post-trial arguments suggest, the Court did not address the possibility that the packets received from the "computing device" in the first network might not have originated from that device. That point is well taken, as common technical definitions of "computing device" lend themselves to a broader understanding that also encompasses, most notably, routers and

[3] Contrary to Centripetal's argument, the Court did not view the '193 Patent claims as *requiring* filtration of packets from a single computer in a first network. Rather, this framing was used because it aligned with the arguments the parties presented at trial. *See, e.g.*, Tr. 869:6–12; Op. at 22 (depicting PTX-563 at 415). The Court also did not "assume that each network described in the claims contains just a single computer." Mem. in Supp. at 7. The Court recognized that networks are made up of many different network devices; its reference to a computing device in the network simply tracked the claim language. *See, e.g.*, Op. at 11; '193 Patent at 14:5–6 ("receive, from a computing device located in a first network, a plurality of packets . . . .").

switches. *See, e.g.*, *Computing Device*, Computer Security Resource Center, Nat'l Inst. of Standards & Tech., https://perma.cc/LE82-YSWP (defining "computing device" as "[a] machine (real or virtual) for performing calculations automatically (including, but not limited to, computer, servers, routers, switches, etc.")). Therefore, since a "computing device" in the first network could be understood by a person of ordinary skill in the art to be a device that forwards packets from multiple endpoint computers in the first network, it is possible that the portion of first network packets described in the claim language contains packets that originated from multiple endpoint computers in the first network.

In that circumstance, blocking the SGT-tagged packets received by the first network computing device may not mean blocking *all* packets from that device—some of the packets may not be tagged (because they may not have originated from computers subject to quarantine). Centripetal appears to insist this "subset" is a "particular type of data transfer" and therefore the Accused Switches and Routers infringe. The Court disagrees, however, and finds that this argument requires a further elaboration of the plain and ordinary meaning of "particular type of data transfer."

In order to do so, the Court consults relevant technical dictionaries. *See CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002) ("[D]ictionary definitions may establish a claim term's ordinary meaning."). The McGraw-Hill Dictionary of Scientific and Technical Terms defines a "data transfer" as "[t]he technique used by the hardware manufacturer to transmit data from computer to storage device or from storage device to computer; usually under specialized program control." *McGraw–Hill Dictionary of Scientific and Technical Terms* 550 (6th ed. 2003). Further, Merriam-Webster's relevant definitions for "type" include "a particular kind, class, or group" and "something distinguishable as a variety." *Merriam-Webster's Collegiate Dictionary*

1354 (11th ed. 2020). Accordingly, since a key distinguishing feature of a data transfer is the technique it employs, the plain and ordinary meaning of "particular type of data transfer" refers to the specific technique, or method, associated with the data transmission.

Therefore, regardless of whether the packets originated from the computing device, or were instead forwarded by the device from multiple endpoint computers in the first network, the "particular type of data transfer" claim limitation is not met. The problem with Centripetal's argument is that a quarantine SGT tag appended to a packet does not specify the technique or method of data transmission associated with that packet. Instead, the evidence shows that the quarantine SGT tag is applied to *all* packets transmitted from a quarantined computer, regardless of the type of transfer. *See* Op. ¶ 17. Centripetal's alternative reading—that SGT-tagged packets are themselves a particular type of data transfer—improperly focuses on the origin of the transfer (*i.e.*, the quarantined computer or group of computers), rather than the specific technique or method of the transfer. And even if this were a possible way to interpret the dictionary definitions, the specification clearly refers to the usage the Court adopts. *Id.* at 25–26 (discussing the specification); '193 Patent at 2:43–54 (explaining filtration method that would "allow users to surf (e.g., GET) to one or more websites attached to the Internet," but prevent riskier types of data transfers associated with exfiltration, such as "users . . . writing (e.g., PUT) data files or posting (e.g., POST) forms to one or more websites"). This confirms the Court's interpretation of the plain and ordinary meaning of the term (based upon dictionary definitions) and indicates that such a reading is not contrary to the '193 Patent disclosure. *See Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1250 (Fed. Cir. 1998) (noting that one should not use a "common meaning" or definition from a "relevant dictionary" to determine the ordinary meaning of a claim term if it would fly "in the face of the patent disclosure").

For these additional reasons, Centripetal has failed to prove infringement of the '193 Patent by a preponderance of the evidence.

2. Reopening the Record

In the alternative, Centripetal requests that if the Court declines to adopt its interpretation of the claim language, it should reopen the record to allow Centripetal to present additional infringement evidence. Mem. in Supp. at 9–11. Centripetal asserts that when it "determined that no further record supplementation was necessary, it did not have notice of the Court's narrowed interpretation of the claims, which departed from the plain and ordinary meaning and thus prejudiced Centripetal." *Id.* at 9.

As discussed above, the Court's interpretation of "particular type of data transfer" does not diverge from the term's plain and ordinary meaning. And Centripetal's assertion that it structured its case based on a "settled understanding" that SGT-tagged packets constitute a "particular type of data transfer" is contrary to the record. *Id.* at 2. Centripetal never requested the Court construe the term and, importantly, has not held a consistent position on the term's meaning. In fact, as the Court recounted in its Opinion, certain of Centripetal's arguments align with the Court's understanding of the term. *See, e.g.*, Op. at 28 (quoting Centripetal PFF ¶ 160) ("[The Accused Switches and Routers] are designed to implement quarantine rules based on detecting abnormal behavior in a variety of data transfer types, including Hypertext Transfer Protocol (HTTP), HTTP GET, and HTTP POST."). Likewise, Cisco has consistently taken the position, from the 2020 trial through the Rule 63 proceedings, that "particular type of data transfer" refers to the method of the transfer. *See, e.g.*, Tr. 2355:4–22, 2362:9–2363:3, 2370:12–2372:25, 2375:2–2377:1, 2387:2–13, 2404:23–2405:16; 2423:25–2424:15; 2425:17–2426:21; 3274:10–3280:20; Rule 63 Tr. 297:8–25,

301:1–304:21, 314:8–14.[4] Centripetal has had ample opportunity to raise this issue; doing so for the first time in its post-trial motion is impermissible. *See Enovsys LLC v. Nextel Commc'ns, Inc.*, 614 F.3d 1333, 1344 (Fed. Cir. 2010) (finding claim construction argument raised for the first time post-judgment was waived when the party had "never requested the district court construe" the term or "offer[] a construction of the term").

The authorities Centripetal relies on in support of its position are far different from this case. Centripetal principally cites to *Wi-Lan, Inc. v. Apple, Inc.*, 811 F.3d 455, 464 (Fed. Cir. 2016). There, the Federal Circuit found that a district court erred in its post-trial ruling on a motion for judgment as a matter of law when it vacated the jury's verdict of invalidity by applying a construction of a claim term that differed from the Court's previous construction of the term. *Id.* at 464–65. Here, of course, there was no construction for the Court to modify. Centripetal also cites instances where courts have granted a new trial when a litigant presented a new theory of liability at trial. *Twigg v. Norton Co.*, 894 F.2d 672, 675–76 (4th Cir. 1990); *Becton Dickinson & Co. v. Tyco Healthcare Grp. LP*, No. Civ.A. 02-1694 GMS, 2006 WL 890995, at *12 & n.7 (D. Del. Mar. 31, 2006). These cases are even farther off the mark, as it is Centripetal who now seeks to raise new theories of liability *post*-trial.

The Court adopted the plain and ordinary meaning of "particular type of data transfer"—a meaning that, at times, Centripetal embraced. Centripetal makes no compelling argument for the Court to reopen the record.

[4] "Tr." refers to the trial transcript. ECF Nos. 496–550. "Rule 63 Tr." refers to the transcript from the Rule 63 hearing. ECF Nos. 750, 753–44.

3. Factual Findings

Centripetal also alleges that the Court's opinion "rests on erroneous factual findings about the functionality of Cisco's Switches and Routers." Mem. in Supp. at 11. Centripetal points to the Court's factual finding that "if the accused devices receive a packet containing a quarantine SGT tag, the devices apply the quarantine SGACL rule and forward or drop the packet depending on whether it is destined for a restricted destination as specified by the ACL rules." Op. ¶ 15; Mem. in Supp. at 11–13. Centripetal maintains that this "description elides the complex series of operations that these devices perform," noting that the devices check the destination of the packet before applying SGACLs. Mem. in Supp. at 12. Because of this, argues Centripetal, "the Court's finding that SGACLs are only destination-based cannot be correct." *Id*.

Centripetal's "destination-based" argument misconstrues the Court's factual finding and does not identify any clear error in need of correction. Centripetal claims that the Accused Switches and Routers engage in more than a "simple destination check" when effecting a quarantine because they make decisions "based on the particular type of data transfer." Reply at 6, ECF No. 808. In support, Centripetal cites evidence showing that the Accused Routers and Switches use SGT tag information when making forward/drop decisions. *Id.* at 8. But the Court explicitly described this functionality (use of SGT tag information) in the factual finding that Centripetal disputes. *See* Op. ¶ 15. Thus, although couched as a factual error, Centripetal's argument here is simply a repackaging of its earlier argument that SGT-tagged packets constitute a "particular type of data transfer." As discussed above, the Court has rejected this legal argument and Centripetal fails to otherwise identify any clear error of fact. *See supra* Part II.A.1.

Centripetal's Motion is denied as to the '193 Patent.

B. '806 Patent

In its Opinion, the Court found that Centripetal failed to meet its burden to establish that Cisco's Accused Switches, Routers, and Firewalls infringed claims 9 and 17 of the '806 Patent. Op. at 37–44. Claim 9 provides that based on "instructions . . . executed by at least one processor," the system "receive[s] a first rule set and a second rule set," "preprocess[es]" both rule sets, and "configure[s] at least two processors . . . to process packets in accordance with the first rule set." '806 Patent at 11:18–29. Then, the system "receive[s] . . . packets" and "process[es], in accordance with the first rule set, a portion of the . . . packets." *Id.* at 11:29–35. Next, in order to effectuate the rule swap, the system "signal[s] each processor . . . to process packets in accordance with the second rule set," and "responsive to being signaled," "configure[s] each processor" to take a series of actions. *Id.* at 11:35–53. Specifically, the processors are configured to "cease processing of one or more packets" and "cache the one or more packets," and the system then "reconfigure[s] [the processor] to process packets in accordance with the second rule set." *Id.* Once reconfiguration is complete, the system "signal[s] completion of reconfiguration," and "responsive to receiving signaling," "process[es], in accordance with the second rule set, the one or more [cached] packets." *Id.* at 11:45–53. Claim 17 describes the same technique. *Id.* at 12:32–64; *see also* Op. ¶ 23.

The Court concluded that Cisco's accused devices did not use this rule swap technique. It recognized that the devices "all cease processing packets, albeit very briefly, and use a form of a queue or buffer to store packets prior to processing." Op. at 37. However, it found that the evidence did not show these actions were taken "responsive to being signaled to process packets in accordance with [a] second rule set." *Id.* at 37–38. Instead, it determined that the evidence showed the cease processing and queue/buffer functionality "occurred as a part of normal packet processing in Cisco's accused devices." *Id.* at 38–39.

In its post-trial motion, Centripetal contends that the Court erred in (1) finding that the "responsive to" element was not met; (2) interpreting the "cease processing" element to require a ceasing of all packet processing; and (3) comparing the accused products to the specification, rather than the language of the claims. Mem. in Supp. at 15.

1. "Responsive to"

Centripetal first argues that the Court misunderstood how the accused Cisco products function and therefore misconstrued Centripetal's infringement argument. Mem. in Supp. at 15–19; Reply at 8–12. Centripetal's argument focuses on the "responsive to" element, asserting that the accused devices meet this requirement because they "receive a signal that causes them to switch from their normal packet processing mode to a rule-swapping state in which they cache packets (to avoid dropping them)." Reply at 11.

In finding that Centripetal failed to establish a causal relationship between the "signal . . . to process packets in accordance with the second rule set" and the cease/cache functions, the Court credited the testimony of Cisco engineers, who explained that the accused devices cease processing packets and cache/buffer packets irrespective of whether a rule swap is occurring. *See* Op. at 38–39. In other words, the evidence showed that "the ceasing and caching of packets . . . occurr[ed] *during* a rule swap, rather than because of it." *Id.* at 38. Specifically, as to the Accused Switches and Routers, Cisco engineer Peter Jones noted that the devices swap from an old rule set to a new one during the existing "two or four internal clock periods" between packet processing. Tr. 2554:20–24. Mr. Jones also testified that while all packets are held in a packet buffer to await processing in the ordinary course, this buffer has no relationship to the accused Hitless ACL rule swap technique. Tr. 2563:10–19. He likewise explained that packet buffering in the Accused Switches operates the same way for all packets and regardless of whether the device is conducting

a rule swap. Tr. 2563:7–19. Similar testimony was provided by Cisco engineer Hari Shankar with respect to the Accused Firewalls and the Transactional Commit Model update technique. Tr. 2521:6–12, 2525:2–17.

In contesting the Court's finding, Centripetal introduces a new concept—the "mode" in which the accused devices are operating. Centripetal argues that unlike "normal packet processing," the rule-swapping mode "causes a signal to cache packets that would otherwise be dropped by default." Reply at 11. Centripetal argues that "the Court erred by assessing how Cisco's products operate in their normal mode, during which there is an extremely brief 'idle period' between the processing of each packet, instead of how they work in the special rule-swapping mode where there is no such idle period and the products cache packets (to avoid dropping them) while a new rule set is substituted for an older set." Reply at 8–9; *see also* Mem. in Supp. at 18 ("By focusing on 'idle' time during normal processing rather than on what occurs during the rule swap process, the Court mistook Centripetal's infringement case.").

This "mode" concept is entirely new, was not previously raised or discussed, and finds no support in the record. It also suggests that Centripetal is now disputing, for the first time, the explanation provided by the Cisco engineers regarding how the accused devices operate. For example, the claim that there is no "idle period" when packets are being swapped directly conflicts with the testimony of Mr. Jones, who explained that this is precisely when the rule swap occurs. *See* Tr. 2554:22–24 ("So in our system it's a fixed time pipeline, so there will be a packet every two or four internal clock periods. And the switch happens between those."). It similarly conflicts with Mr. Shankar's testimony regarding the operation of the firewalls. Op. ¶¶ 33–36. It also comes in stark contrast to Centripetal's previous position that the Cisco engineer testimony supported its

theory of infringement. For example, Centripetal directly quoted the following section of Mr. Jones's cross-examination in its trial brief as support for the '806 Patent cease and cache elements:

> Q. And then during the two to four clock periods that you mentioned yesterday, when there's no processing of packets, the rules are swapped; isn't that right?
> A. That is correct. There is -- the processing of packets continues. Packets are processed at a maximum frequency of two to four clock periods. So we don't stop processing the packets, there's just an idle period between two packets.
> Q. But there's a signal that's sent to say, stop processing packets with the old rule set and start processing packets with the new rule set, correct?
> A. Yes, we swap from the old to the new.
> Q. And you do that swap in between -- in that two to four clock cycles that you mentioned yesterday, correct?
> A. Right.

Pl. Centripetal Networks, LLC's Trial Br. at 12, ECF No. 703 (quoting Tr. 2572:7–20). To the extent Centripetal believed that the engineers were improperly discussing "normal mode," rather than "rule-swapping mode" in their testimony, it never raised such an issue and instead chose to rely on the testimony in support of its arguments.

Centripetal also cites to various statements made by its expert, Dr. Mitzenmacher. The Court considered the testimony of Dr. Mitzenmacher and found that he "did not clearly offer an opinion as to th[e] causal relationship" between the "signal[] to process packets in accordance with the second rule set" and the ceasing processing and caching of the packets. *See* Op. at 38 (citing Tr. 601:23–25, 627:19–25, 707:11–12, 707:19–20). The Court likewise addressed Centripetal's argument that one could infer causation because Cisco's "new rule update techniques were designed to avoid dropping packets." *Id.* at 39. Dr. Mitzenmacher opined that the no-dropped-packets functionality indicated to him that the accused devices would need to cease processing packets during a rule swap. *Id.* at 39 (citing Tr. 634:7–14, 706:3–5). Dr. Mitzenmacher also drew a connection between the lack of packet drops and the devices' use of a packet buffer during a rule swap. *Id.* at 39–40 (citing Tr. 641:18–24, 712:17–23). However, the Court did not find this

persuasive, noting that "[e]ven though a rule swap technique might be able to take advantage of . . . existing functionality to avoid dropped packets, this does not mean that the ceasing and caching operations are done 'responsive to' the rule swap." *Id.* at 40. For these reasons, Centripetal fails to establish "a clear error of law" or "manifest injustice" warranting relief as to this issue. *P. Ins. Co.*, 148 F.3d at 403.

2. "Cease Processing"

Next, Centripetal argues that the Court misconstrued the term "cease processing of one or more packets." Mem. in Supp. at 19. The Court understood the plain and ordinary meaning of this term to require the system to stop processing packets entirely. Op. at 42–44. Centripetal maintains this was an error and that "cease processing" should be construed instead to mean "stop processing packets" in a specific way, namely "with the old rule set." Mem. in Supp. at 19 (emphasis omitted). Centripetal cites to embodiments in the specification that it argues require such a limitation. *Id.* Further, Centripetal argues that the Court improperly treated an embodiment in the specification (Figure 4) as a limitation on the claims. *Id.*

It is Centripetal, not the Court, that seeks to impermissibly use the specification to modify the claim language. The Court did not treat an embodiment in the specification (Figure 4) as a limitation on the claims. It merely referenced Figure 4 as being consistent with its plain language analysis—that "cease processing of one or more packets" means that the system stops processing packets entirely. *See, e.g., Accent Packaging, Inc. v. Leggett & Platt, Inc.*, 707 F.3d 1318, 1326 (Fed. Cir. 2013); Op. at 42–43. Further, the Court rejects Centripetal's suggestion that the specification can be used to modify abundantly clear claim language. *See Buckingham Mfg. Co. v. Bashlin Indus., Inc.*, No. 2:21-cv-1390, 2022 WL 17668809, at *14 (W.D. Pa. July 8, 2022)

(rejecting construction that "adds words to the claims that are not present"); *Leviton Mfg. Co. v. Universal Sec. Instruments, Inc.*, 304 F. Supp. 2d 726, 739 (D. Md. 2004) (similar).

3. Comparing Accused Products to Specification

Lastly, Centripetal argues that the Court improperly relied on the patent specification. Centripetal points to the Court's observation that Cisco's accused devices do not solve a problem described in the specification, namely, "processing packets in accordance with an outdated rule set." Mem. in Supp. at 20. It argues this was "not the right comparison" because "[t]he only issue for infringement is whether the accused products meet the claims; whether they meet the specification is irrelevant." *Id.* at 20–21 (emphasis omitted). The Court's non-infringement conclusion does not rely on this analysis. Rather, the Court noted that this fact "further supported" its findings in order to provide additional context.[5] Op. at 44.

Centripetal's Motion is denied as to the '806 Patent.

C. '176 Patent

In its Opinion, the Court found that Centripetal failed to meet its burden to establish that Cisco's Accused Switches and Routers infringed claims 11 and 21 of the '176 Patent. Op. at 53–61. Claim 11 provides that a system "identify a plurality of packets received by a network device from a host located in a first network" and "generate a plurality of log entries corresponding to the plurality of packets *received by* the network device." '176 Patent at 17:10–13 (emphasis added). Likewise, the system is to "identify a plurality of packets transmitted by the network device to a

[5] Centripetal argues that the Court "misinterpreted" the testimony of Cisco engineer Mr. Shankar when it used his testimony to support its position that the specification further supports the Court's non-infringement finding. Mem. in Supp. at 21. Centripetal argues that Mr. Shankar's testimony is "not evidence of non-infringement" because he was discussing "what occurs during normal packet processing." *Id.* This appears to be a species of Centripetal's "mode" argument, addressed above. In any event, the Court's non-infringement finding does not rely on this discussion of the specification.

host located in a second network" and "generate a plurality of log entries corresponding to the plurality of packets *transmitted by* the network device." *Id.* at 17:14–18 (emphasis added). Then, "based on the plurality of log entries corresponding to the plurality of packets received by the network device and the plurality of log entries corresponding to the plurality of packets transmitted by the network device," the system "correlate[s] . . . the plurality of packets transmitted by the network device with the plurality of packets received by the network device." *Id.* at 17:19–25. Finally, "responsive to correlating," the system "generate[s], based on the correlating, one or more rules configured to identify packets received from the host located in the first network," and "provision[s] a device located in the first network with the one or more rules." *Id.* at 17:26–35. These steps are the same for claim 21. *Id.* at 18:63–19:23; *see also* Op. ¶ 45.

The Court found that the preponderance of the evidence did not establish that Cisco's Accused Switches and Routers use this packet correlation technique. Op. at 53–54. Specifically, the Court found that Centripetal did not present evidence that Cisco's accused devices "correlate . . . the plurality of packets transmitted by the network device with the plurality of packets received by the network device" based on the ingress and egress log entries corresponding to those sets of packets. Op. at 53–59; *see* '176 Patent at 17:19–25. Instead, the Court found that the evidence showed the accused devices conducted a different kind of correlation—between internal NetFlow log records or proxy data and external threat behaviors. Op. at 57. The Court likewise found that Centripetal did not demonstrate that "responsive to correlating," the devices "generate, based on the correlating, one or more rules configured to identify packets received from the host located in the first network" and "provision a device" with those rules. Op. at 60; *see* '176 Patent at 17:26–35. The Court opined that "[w]hile the evidence shows that the system generates alerts, these alerts

are not 'rules,'" nor do they have the capability of identifying the packets received from the first network host. Op. at 60.

Centripetal argues that the Court's findings regarding the correlation limitation and the generate and provision limitation were both in error.

1. "Correlate" Limitation

Centripetal raises multiple issues with the Court's finding that Centripetal did not establish that Cisco's accused devices perform the correlation specified in the claims—specifically, a correlation between the "packets received by the network device" with the packets "transmitted by the network device" based on ingress and egress log entries reflecting the received/transmitted packets. Mem. in Supp. at 22–28; *see* Op. at 54; '176 Patent at 17:19–25.

First, Centripetal argues that the Court erred in concluding that Centripetal had failed to establish that Cisco's Stealthwatch correlates ingress and egress NetFlow records. Mem. in Supp. at 23–25. Centripetal argues that the evidence was "undisputed" and that its expert, Dr. Cole, established the correlation limitation using Cisco documents. *Id.* at 23. These same arguments and evidence were previously presented to and considered by the Court. In its Opinion, the Court found that Centripetal had failed to prove the correlation limitation. Op. at 56–59. As the finder of fact, the Court gave the testimony of Dr. Cole "little weight," noting the "paucity and indefiniteness of the evidence [he] relied on." *Id.* at 58. The Court also reviewed and considered the documents relied on by Centripetal in concluding that Centripetal had not met its burden. *Id.* at 56–59. Centripetal fails to point to any clear error and the Court finds no reason to revisit its previous analysis.

Centripetal also claims that the countervailing evidence the Court cited to further support its conclusion does not establish that Stealthwatch is incapable of performing the claimed

correlation. Mem. in Supp. at 23–24. But this argument misses the point. The Court found that Centripetal failed to meet its burden to show the accused devices perform each claim limitation. Cisco was not required to establish non-infringement (*i.e.*, that Stealthwatch does not perform the claimed correlation), and the observation that other documents bolstered the Court's conclusion was appropriate.

Second, Centripetal argues that the Court failed to consider other ways in which the "correlate" element could be met—specifically, through deduplication of NetFlow data and the correlation of NetFlow with other data types, such as Syslogs and WebFlow. *Id.* at 25–27. However, these infringement theories were not presented at trial. As the Court noted in its Opinion, at trial, Centripetal only presented testimony from its expert, Dr. Cole, on Stealthwatch's alleged correlation of ingress and egress NetFlow records. Op. at 55 (citing Tr. 993:19–999:15, 1102:16–1103:4, 1106:5–8, 1108:1–5). Dr. Cole never discussed deduplication and noted that his infringement opinion did not involve a proxy, meaning that any correlation by Stealthwatch of Syslogs or WebFlow—which Centripetal has indicated are generated by proxy sources—does not support Dr. Cole's infringement analysis. *Id.* (quoting Tr. 978:11–18). Further, Centripetal chose not to supplement the record or recall witnesses in the Rule 63 proceeding. Pl.'s Notice at 1–2. Instead, it asked the Court to rule based on the trial record that was developed before Judge Morgan. *Id.* As such, the Court finds that these new infringement theories, which are largely undeveloped in the record and lack supporting expert testimony, are unpersuasive based on the record before the Court, and further supplementation is improper at this stage.

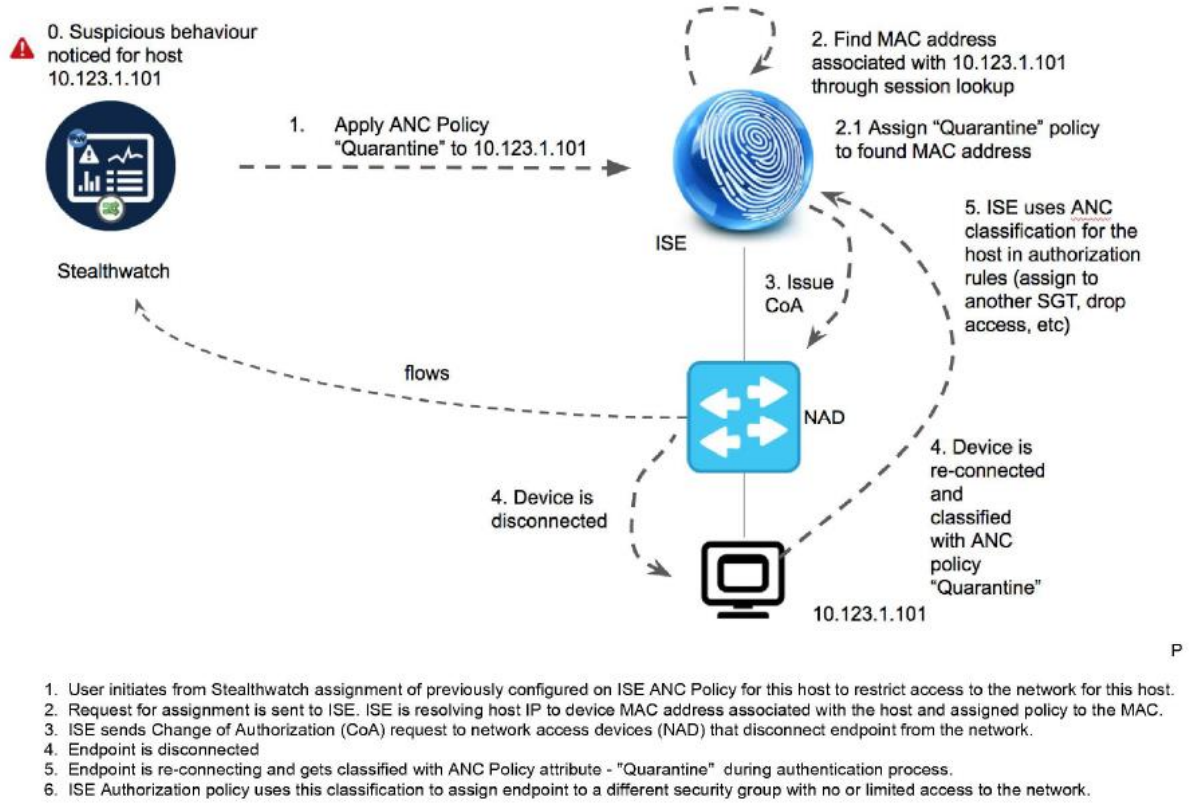
Third, Centripetal claims that the Court improperly "compared the accused products to the discussion of packet obfuscation in the patent specification rather than applying the asserted claims." Mem. in Supp. at 27. Contrary to Centripetal's contentions, the Court did not "require

packet obfuscation as one of the [claim] limitations." Mem. in Supp. at 28. The Court's evaluation of Centripetal's evidence related to the correlate element did not discuss packet obfuscation. The Court merely referenced the specification at the end of its analysis to provide context and to highlight that its conclusion was consistent with the fact that "the Accused Switches and Routers do not have the problem that the '176 Patent was designed to solve." Op. at 59.

2. Generate and Provision Limitation

Next, Centripetal argues that the Court erred in concluding that Stealthwatch, based on the correlation, does not generate rules "configured to identify packets received from the host located in the first network" or "provision[] a device" with those rules. Mem. in Supp. at 28 (quoting '176 Patent at 17:26–35). The parties agreed that "rule" means "a condition or set of conditions that when satisfied cause a specific function to occur." Op. & Order ("*Markman* Order") at 9, ECF No. 202.

Centripetal, similar to its previous arguments, asserts that Stealthwatch generates a "rule" "when it creates a policy update to initiate the quarantine." Mem. in Supp. at 28; *see also* Centripetal PFF ¶ 372 ("Stealthwatch will respond to identified threats to generate rules that are sent to the Catalyst 9000 Switch and ISR/ASR Router to block specific packets that were identified to be threats."). In its Opinion, the Court rejected this argument, finding that while Stealthwatch generates alerts, these do not, in and of themselves, "cause a specific function to occur." Op. at 60. Here, Centripetal contests this finding, claiming that the Court "misstated the operation of the Stealthwatch," because "Stealthwatch . . . automatically generates the rule in response to the correlating of NetFlow and then propagates the responsive rule." Mem. in Supp. at 29. In support, Centripetal principally relies on the following diagram from a Cisco technical document:



PTX-1089 at 1238.

At trial, Centripetal's counsel asked its expert, Dr. Cole, about this diagram. Dr. Cole was asked, "[s]o what happens when they realize that there's some suspicious behavior noticed for the host?" Tr. 1002:11–12. Dr. Cole responded that "[i]t can go in and send a policy, which can also be thought of as rules, to take some action, in this case to quarantine a specific IP address." Tr. 1002:13–15. But as the Court previously explained, the quarantine function does not occur absent human intervention. Op. at 60. Centripetal's focus on step one of the diagram, "Apply ANC Policy 'Quarantine,'" does not change that conclusion. As the explanation for step 1 below the diagram makes clear, the quarantine action is not automatically triggered from Stealthwatch alerting suspicious network behavior; instead, the quarantine is "initiat[ed]" by the "[u]ser." PTX-1089 at 1238. Moreover, as detailed after the diagram, the "interaction between the user and the system" involves the user, "Adam the Analyst," "notic[ing] the alert and open[ing] Host Report for the host

to investigate host details," "decid[ing] to limit access to the network for the host via ISE ANC," "review[ing] if there are any ANC Policy already assigned to the host," and "open[ing] ANC options available for the host and select[ing] ISE and ANC Policy appropriate for assignment," all before "Stealthwatch sends assignement [sic] request to ISE and notif[ies] Adam if request is successfull [sic] and policy is assigned or any error occurred." *Id.* at 1238–39. Therefore, even if the Court found that Stealthwatch practiced the claimed correlation (which it did not), the result of that correlation—the identification and alert of suspicious behavior—is not a "rule" because it does not "cause a specific function to occur" (*e.g.*, the quarantine of a particular IP address), without significant human interaction. *See Markman* Order at 9; '176 Patent at 17:26–35.[6]

Finally, Centripetal takes issue with the Court's finding that, even setting aside the human inputs necessary to generate a rule, Centripetal "has not shown that the rules that would be created based on a Stealthwatch alert would have the ability to 'identify packets received from the host located in the first network.'" Op. at 60; Mem. in Supp. at 30. Centripetal argues, and Court agrees, that the Stealthwatch alert can identify a suspicious host in a network. Mem. in Supp. at 30; PTX-1089 at 1238. However, it is not clear why such alerts have any relationship to identifying packets received by the network device from a host in the first network, as distinguished from packets transmitted by the network device to a host in a second network. In any event, Centripetal's failure to prove multiple other claim limitations would prohibit relief.

---

[6] In its *Markman* Order, the Court adopted the plain and ordinary meaning of "generate, based on the correlating, one or more rules." *Markman* Order at 19–20. In so doing, the Court rejected a narrower construction proposed by Cisco that automated rule generation be "based on the correlating, not based on user defined filters or rules." *Id.* Centripetal argues that this ruling supports its argument that the quarantine rules can satisfy that claim limitation. Mem. in Supp. at 30. However, Centripetal's argument conflates two distinct requirements: (1) that the "system . . . generate . . . one or more rules," and (2) that such rules be "based on the correlating." '176 Patent at 17:8–9, 29–31. Regardless of what the rules are "based on," the claims describe a *system* that "generate[s]" rules. *See id.* The quarantine rules, as made plain above, are not system generated.

Centripetal's Motion is denied as to the '176 Patent.

III. CONCLUSION

For the reasons set forth above, Centripetal's post-trial motion is DENIED. ECF No. 787. The Clerk is DIRECTED to send a copy of this Order to all counsel of record.

It is so ORDERED.

/s/
Elizabeth W. Hanes
United States District Judge

Date: June 14, 2024